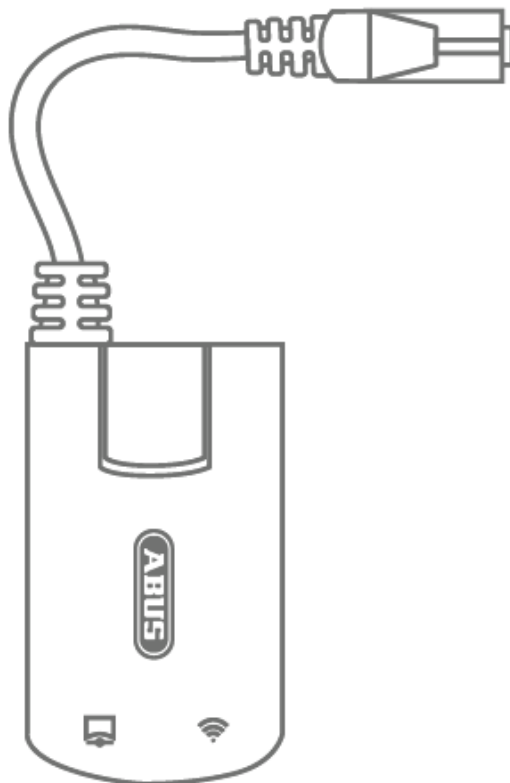


# FUMO50040

## Secvest WIFI-Modul



DE

### Secvest WIFI-Modul

Installations- und Bedienungsanleitung

EN

### Secvest Wi-Fi module

Installation instructions and user manual



## Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b> .....	<b>2</b>
<b>Einführung</b> .....	<b>4</b>
Hinweise zur Bedienungsanleitung .....	4
Bestimmungsgemäße Verwendung .....	4
Haftungsbeschränkung .....	4
<b>Sicherheitshinweise</b> .....	<b>5</b>
Symbolerklärung .....	5
Verpackung .....	5
<b>Lieferumfang</b> .....	<b>5</b>
<b>Technische Daten</b> .....	<b>6</b>
<b>Funktionsprinzip und Leistungsmerkmale</b> .....	<b>7</b>
Allgemeines .....	7
Hauptmerkmale .....	7
Position und Einbau .....	7
LEDs .....	9
Erforderliches Equipment .....	9
Werkseinstellungen .....	9
<b>Konfiguration</b> .....	<b>10</b>
Schritt 1: Einloggen .....	10
Schritt 2: Erste Verbindung zum Router .....	11
Schritt 3: Weitere Verbindungen zum Router .....	16
<b>Systemeinstellungen</b> .....	<b>17</b>
Nutzernamename und Passwort .....	17
Firmware Upgrade .....	18
<b>Netzwerk Einstellungen</b> .....	<b>19</b>
Lokaler Netzwerk-Anschlussstyp .....	19
<b>Weitere Informationen zu WLAN und Routern</b> .....	<b>21</b>
Zwei Wi-Fi Access Points mit identischer SSID / identischem Passwort, Administrator .....	21
Signalstärke-Entscheidungsfindung .....	22
DHCP / Feste IP Adresse .....	23
Automatische Kanalwahl .....	23
Bandsteuerung .....	24
<b>Gewährleistung</b> .....	<b>25</b>
<b>Kundendienst und Support</b> .....	<b>25</b>
<b>Entsorgung</b> .....	<b>26</b>
<b>Konformitätserklärung</b> .....	<b>26</b>
<b>Contents</b> .....	<b>28</b>
<b>Introduction</b> .....	<b>30</b>
Information on user guide .....	30
Intended use .....	30

Limitation of liability.....	30
<b>Safety information.....</b>	<b>31</b>
Explanation of symbols.....	31
Packaging.....	31
<b>Scope of delivery .....</b>	<b>31</b>
<b>Technical data .....</b>	<b>32</b>
<b>Functional principle and features.....</b>	<b>33</b>
General .....	33
Main features .....	33
Position and installation .....	33
LEDs .....	35
Required equipment .....	35
Default settings .....	35
<b>Configuration.....</b>	<b>36</b>
Step 1: Logging on.....	36
Step 2: Initial connection to router .....	37
Step 3: Additional connections to the router .....	41
<b>System settings.....</b>	<b>42</b>
User name and password.....	42
Firmware upgrade.....	43
<b>Network settings .....</b>	<b>44</b>
Local network connection type .....	44
<b>More information about Wi-Fi and Routers.....</b>	<b>46</b>
Two Wi-Fi Access Points with Identical SSID/Password, Administrator .....	46
Signal Strength Decision Making.....	47
DHCP / Fixed IP address.....	48
Auto Channel selection.....	48
Band Steering .....	49
<b>Warranty.....</b>	<b>50</b>
<b>Customer service and support .....</b>	<b>50</b>
<b>Disposal .....</b>	<b>51</b>
<b>Declaration of conformity.....</b>	<b>51</b>

## Einführung

### Hinweise zur Bedienungsanleitung

Sehr geehrte Kundin, sehr geehrter Kunde,

wir bedanken uns bei Ihnen für den Kauf dieses Produkts. Mit diesem Gerät haben Sie ein Produkt erworben, das nach dem heutigen Stand der Technik gebaut wurde.

Diese Anleitung enthält wichtige Hinweise zur Inbetriebnahme und Handhabung. Beachten Sie die Anweisungen und Hinweise in dieser Anleitung um einen gefahrlosen Betrieb sicherzustellen. Heben Sie diese Anleitung zum Nachlesen auf. Diese Anleitung gehört zum Gerät. Wenn Sie das Gerät an Dritte weitergeben, vergessen Sie bitte nicht, auch diese Anleitung mit auszuhändigen.

### Bestimmungsgemäße Verwendung

Verwenden Sie das Gerät ausschließlich für den Zweck, für den es gebaut und konzipiert wurde! Jede andere Verwendung gilt als nicht bestimmungsgemäß. Dieses Produkt erfüllt die Anforderungen der geltenden europäischen und nationalen Richtlinien.

Die Konformität wurde nachgewiesen, die entsprechenden Erklärungen und Unterlagen sind beim Hersteller hinterlegt.

Um diesen Zustand zu erhalten und einen gefahrlosen Betrieb sicherzustellen, müssen Sie als Anwender diese Bedienungsanleitung beachten! Bei Fragen wenden Sie sich an Ihren Fachhändler. Allgemeine weiterführende Hinweise und Hinweise zum Produkt-Support finden Sie auf [www.abus.com](http://www.abus.com) auf der allgemeinen Seite oder für Händler und Installateure im Partnerportal.



#### Hinweis

Beachten Sie die Anweisungen und Hinweise in dieser Anleitung! Sollten Sie sich nicht an diese Anleitung halten, erlischt Ihr Garantieanspruch! Für Folgeschäden wird keine Haftung übernommen!

Das gesamte Produkt darf nicht geändert oder umgebaut werden.

Bitte beachten Sie die lokalen gesetzlichen Bestimmungen. In einigen europäischen Ländern ist der Einsatz von Repeatern im Außenbereich verboten oder die max. Alarmdauer ist begrenzt. Informieren Sie sich hierzu bei den lokalen Behörden.



#### Gefahr

Bevor Sie mit Installations- und Wartungsarbeiten beginnen, setzen Sie die Zentrale in den Errichter Modus. Im Errichter Modus wird verhindert, dass Alarmer aktiviert werden, wenn der Deckel des Repeaters geöffnet wird.

### Haftungsbeschränkung






Es wurde alles Erdenkliche unternommen, um sicherzustellen, dass der Inhalt dieser Anleitung korrekt ist. Jedoch kann weder der Verfasser noch ABUS Security-Center GmbH & Co. KG die Haftung für einen Verlust oder Schaden übernehmen, der durch falsche Installation und Bedienung, bestimmungswidrigen Gebrauch oder durch Nichtbeachtung der Sicherheitshinweise und Warnungen verursacht wurde. Für Folgeschäden wird keine Haftung übernommen. Das gesamte Produkt darf nicht geändert oder umgebaut werden. Sollten Sie sich nicht an diese Hinweise halten, erlischt Ihr Garantieanspruch. Technische Änderungen vorbehalten.

© ABUS Security-Center GmbH & Co. KG, 12/2019


## Sicherheitshinweise

### Symbolerklärung

Folgende Symbole werden in der Anleitung bzw. auf dem Gerät verwendet:

Symbol	Signalwort	Bedeutung
	<b>Gefahr</b>	Warnhinweis auf Verletzungsgefahren oder Gefahren für die Gesundheit.
	<b>Gefahr</b>	Warnhinweis auf Verletzungsgefahren oder Gefahren für Ihre Gesundheit durch elektrische Spannung.
	<b>Wichtig</b>	Sicherheitshinweis auf mögliche Schäden am Gerät/Zubehör.
	<b>Hinweis</b>	Hinweis auf wichtige Informationen.
		Die EU-Richtlinie WEEE 2012/19/EU regelt die ordnungsgemäße Rücknahme, Behandlung und Verwertung von gebrauchten Elektronikgeräten. Dieses Symbol bedeutet, dass im Interesse des Umweltschutzes das Gerät am Ende seiner Lebensdauer entsprechend den geltenden gesetzlichen Vorschriften und getrennt vom Hausmüll bzw. Gewerbemüll entsorgt werden muss. Die Entsorgung des Altgeräts kann über entsprechende offizielle Rücknahmestellen in Ihrem Land erfolgen. Befolgen Sie die örtlichen Vorschriften bei der Entsorgung der Materialien. Weitere Einzelheiten über die Rücknahme (auch für Nicht-EU Länder) erhalten Sie von Ihrer örtlichen Verwaltung. Durch das separate Sammeln und Recycling werden die natürlichen Ressourcen geschont und es ist sichergestellt, dass beim Recycling des Produkts alle Bestimmungen zum Schutz von Gesundheit und Umwelt beachtet werden.

### Verpackung

 Gefahr	Halten Sie Kinder von Verpackungsmaterialien und Kleinteilen fern Erstickungsgefahr!
	Vor dem Gebrauch des Gerätes jegliches Verpackungsmaterial entfernen.

### Lieferumfang

- 1x ABUS Wifi Modul
- 1x DC-DC-Konverter
- 1x Quick Guide
- 1x Sicherheitshinweise
- Montagematerial

## Technische Daten

Produktname	ABUS Wifi Modul
Produktbezeichnung	Wifi Modul
Artikelnummer	FUMO50040
Hersteller	ABUS Security-Center GmbH & Co. KG
Unterstützte Netzwerkverschlüsselung	54/128/WEP encryption; WPA-PSK/WPA2-PSK, WPA/WPA2
Betriebsband	2,4 GHz
Übertragungsgeschwindigkeit	Max. 300 Mbps
Ethernet Kabel Länge	150 mm
Funk	2,4 GHZ; 100mW max.
Betriebstemperatur	-10 °C bis +55 °C
Luftfeuchtigkeit, max.	max. 93 %, nicht kondensierend
Abmessung (BxHxT)	350 x 590x 110 mm
Gewicht	20g (Wifi Modul), 22g (Gleichspannungswandler)
Ausführungsart der Stromversorgung	Ausführungsart W (EN 50131-4:2009 §5.6.3.2)
Stromverbrauch / Energieverbrauch	Max. 220 mA @ 5VDC
Betriebsspannung	5V DC
Gleichspannungswandler	Eingang: Stromaufnahme max. 100 mA @ 12VDC Ausgang: max. 22 mA @ max. 5 VDC

## Funktionsprinzip und Leistungsmerkmale

### Allgemeines

Das WIFI Modul FUMO50040 ermöglicht die drahtlose Netzwerkverbindung von ABUS Zentralen an einen lokalen Netzwerkrouter. Somit wird ein direkter Ethernet-Kabelanschluss zwischen Zentrale und lokalen Netzwerkrouter nicht mehr benötigt. Das WIFI Modul wird direkt über die Zentrale mit Strom versorgt und im Gehäuse intern installiert.

### Hauptmerkmale

Kompatibel mit Secvest Zentrale

Einbau direkt im Secvest Gehäuse

Fungiert als Verbindung zum heimischen Router und ersetzt somit den Anschluss über LAN Kabel

Nicht batteriebetrieben

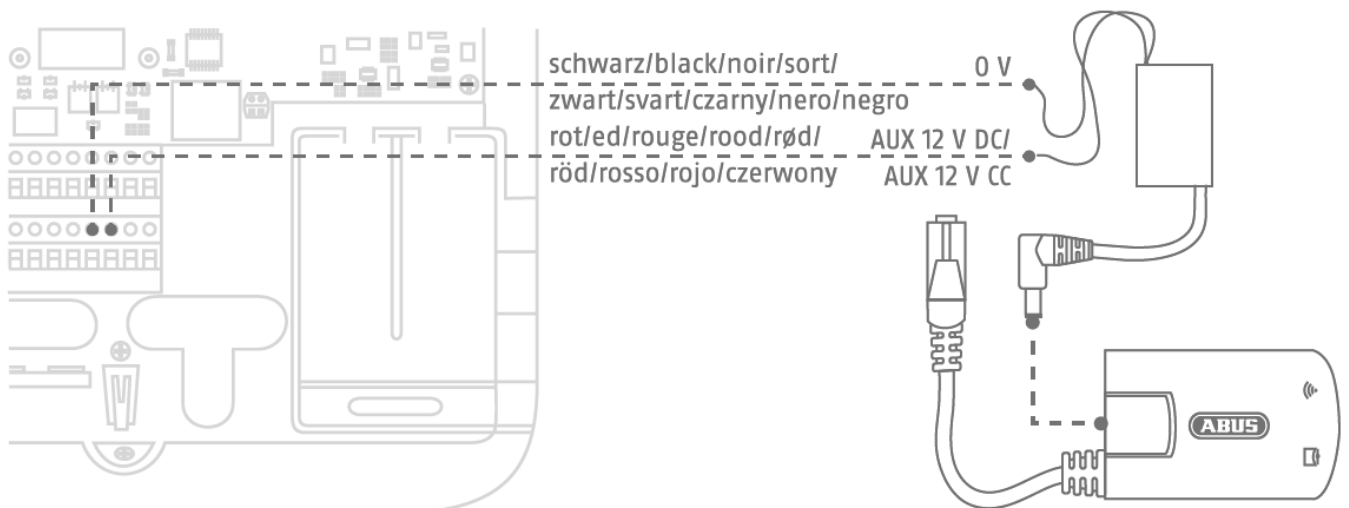


Gefahr

- Bevor Sie mit Installations- und Wartungsarbeiten beginnen, gehen Sie bei der Secvest Zentrale in den Errichter Modus und schalten Sie die Anlage komplett spannungslos!

### Position und Einbau

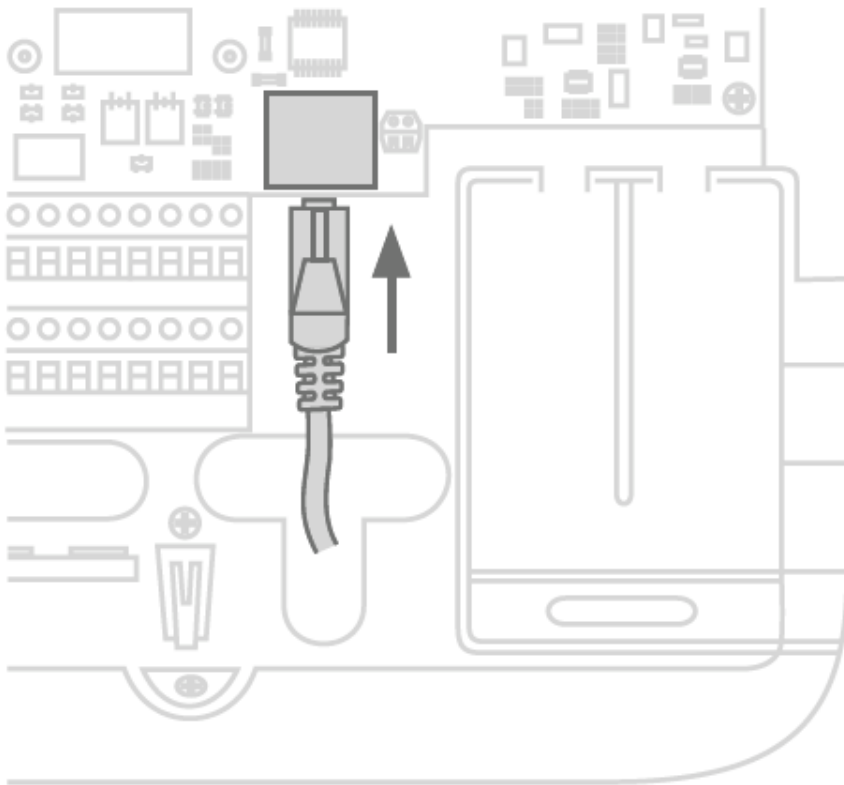
1. Schließen Sie den DC-DC-Konverter an das Wifi Modul an. Schließen sie anschließend das schwarze und das rote Kabel wie in folgender Abbildung an.



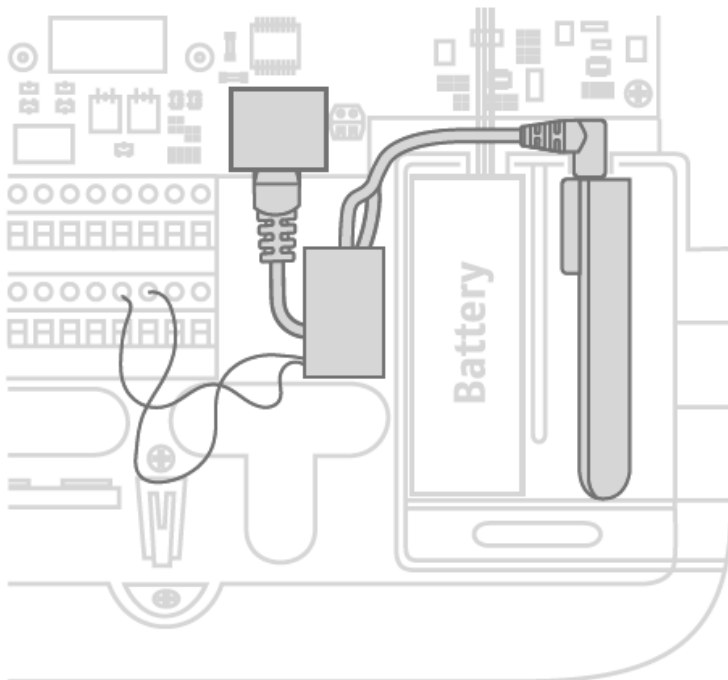
Hinweis

Das Modul darf nicht in der Nähe einer Hitzequelle montiert werden.

2. Schließen Sie das Ethernet-Kabel des Wifi Moduls an



3. Positionieren Sie das Wifi Modul und den Konverter in der Nähe des Ethernet Anschlusses in der Secvest. Ein Positionierungsbeispiel sehen Sie in folgender Abbildung.





### LEDs

Schnell blinkende, blaue LEDs	WLAN-Verbindung zum Router ok
Langsam blinkende, blaue LEDs	WLAN-Verbindung zum Router schlägt fehl
Blinkende, grüne LEDs	LAN-Verbindung

### Erforderliches Equipment

Folgendes wird für die Programmierung des FUMO50040 Wifi-Moduls benötigt:

- Ein WLAN-fähiger Laptop, Smartphone oder Tablet
- WLAN-Passwort des Kunden, um das Modul zu verbinden



Hinweis

Wenn im Objekt weitere WLAN-Repeater sind, diese bitte zuerst ausschalten, bevor der FUMO50040 Wifi-Adapter sich mit dem Hauptrouter verbindet



Hinweis

Prüfen Sie bitte, ob der FUMO50040 Wifi-Adapter mit ihrem Router kompatibel ist (Sky Q Router sind nicht kompatibel)

Wenn der FUMO50040 Wifi Adapter nicht mit dem Router kompatibel ist, verbinden Sie bitte die Zentrale direkt per LAN-Kabel an den Router

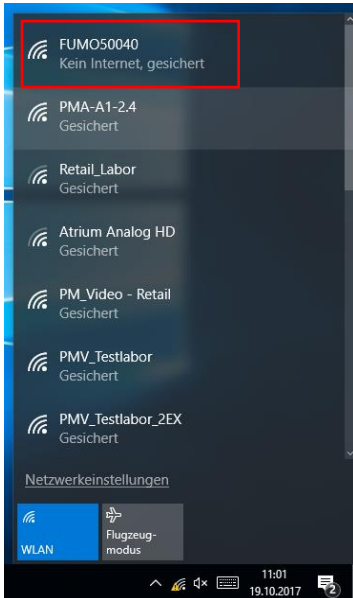
### Werkseinstellungen

- Machen Sie das Wifi-Modul stromlos
- Drücken Sie den „Reset“-Knopf auf der flachen Oberseite des Moduls. Halten Sie diesen gedrückt
- Schließen Sie das Wifi Modul wieder an den Strom an
- Warten Sie ca. 30 Sekunden, bis die blaue LED blink und lassen Sie anschließend den „Reset“-Knopf los
- Das Gerät startet neu. Dies dauert in etwa 2 Minuten

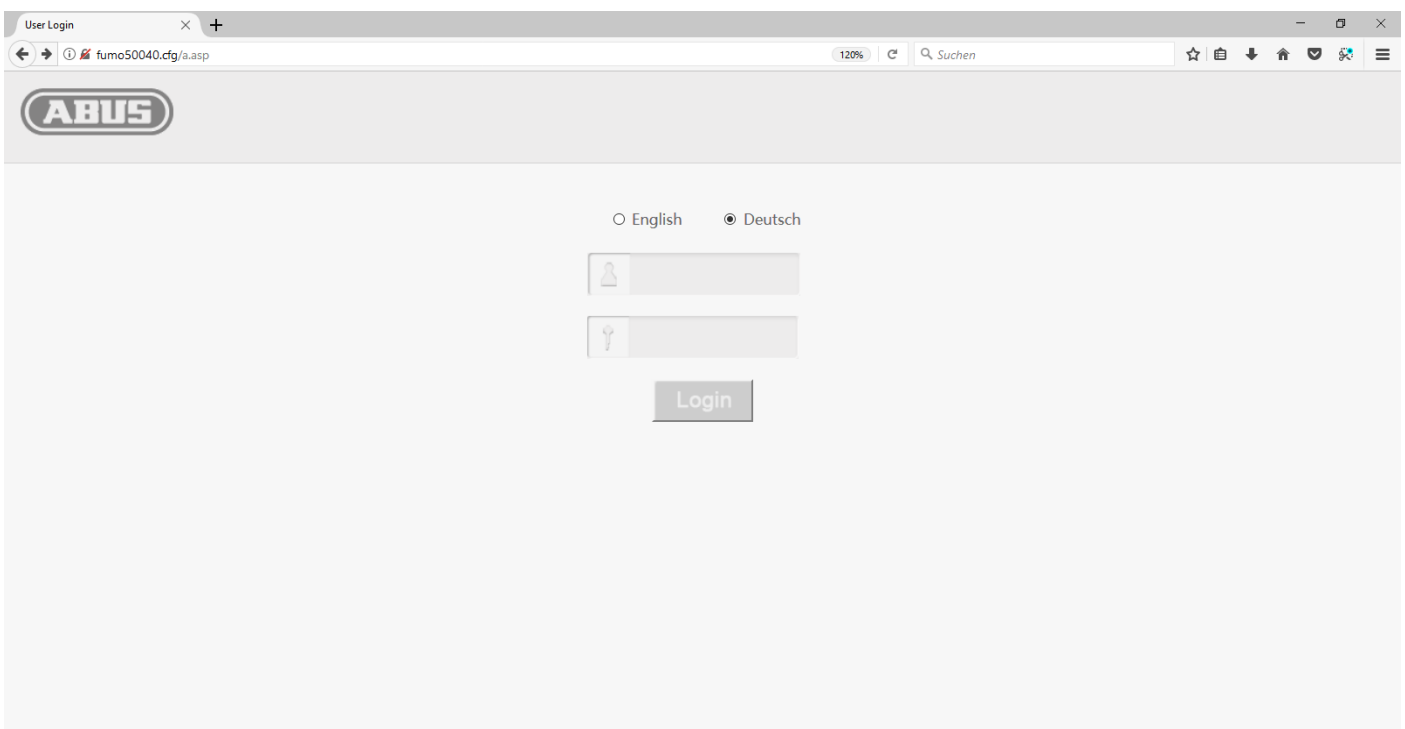
## Konfiguration

### Schritt 1: Einloggen

- Es wird ein WLAN-fähiger Laptop oder eine andere WLAN-fähige Komponente benötigt
- Gehen Sie zu den Netzwerkeinstellungen und verbinden sich mit dem Netzwerk „FUMO50040“
- Das Standardpasswort ist „12345678“.



- Öffnen Sie den Internet-Browser und geben oben in der Adresszeile <http://fumo50040.cfg> ein. Sie kommen auf die Log-In Seite für das Wifi Modul
- Melden Sie sich mit dem Benutzernamen „abus“ und dem Passwort „abus“ an
- Klicken Sie auf „Login“



## Schritt 2: Erste Verbindung zum Router

- Drücken Sie auf den Menüpunkt „Nach Hotspots suchen“.
- Wählen Sie aus der Liste das WLAN-Netzwerk des Kunden aus
- Klicken Sie auf „Weiter“



Hinweis

Wenn im Objekt weitere WLAN-Repeater sind, diese bitte zuerst ausschalten, bevor das FUMO50040 Wifi-Modul sich mit dem Hauptrouter verbindet

ABUS Betriebsart: WiFi Bridge English

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen >>>

Systemeinstellungen

Netzwerkeinstellungen

### WLAN Hotspot

Wählen Sie eine Netzwerk aus, um sich mit diesem zu verbinden. Wenn das gewünschte Netzwerk nicht gefunden wird, laden Sie die Seite erneut oder geben Sie die SSID manuell ein. Danach auf "Weiter" klicken.

SSID	MAC	Kanal	Signal	Auth / Enc
PM_Video - Retail	02:1d:aa:b3:ed:48	12	100	WPA2-PSK / AES
WLAN-ASC	02:a0:57:1b:eb:00	8	96	WPA2 / AES
WLAN-Gast	00:a0:57:1b:eb:00	8	96	WPA2-PSK / AES
PMA-A1-2.4	ec:1a:59:b7:bf:ee	1	96	WPA2-PSK / AES
PMV_Testlabor	00:1d:aa:b3:ed:48	12	91	WPAPSK-WPA2PSK / TKIPAES
PMV_Testlabor_2EX	74:da:38:c0:55:a8	12	86	WPA2-PSK / AES
WLAN-Gast	00:a0:57:1b:f2:de	6	86	WPA2-PSK / AES
WLAN-ASC	02:a0:57:1b:f2:de	6	86	WPA2 / AES

Es gibt 15 Netzwerke

SSID

Liste neu laden

Weiter Beenden

- Wenn das Netzwerk des Routers nicht in der Liste erscheint, klicken Sie auf den Punkt „SSID“ (siehe rote Markierung im Bild)
- Geben Sie das Netzwerk manuell ein



Hinweis

Mit der manuellen Eingabe eines Netzwerkes aus der Liste kommen Sie auch zu den Erweiterten Einstellungen. Siehe Konfiguration Schritt 2b

- Klicken Sie auf „Weiter“

## Schritt 2a: Sicherheitseinstellungen



Hinweis

Diese Ansicht ist bei der Auswahl des Netzwerkes aus der Liste zu sehen.

- Nachdem Sie auf „Weiter“ geklickt haben, folgen die Sicherheitseinstellungen
- Geben Sie das Passwort des Netzwerkes des Heim-Routers ein (Punkt 4).

ABUS Betriebsart: WiFi Bridge English

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen >>>

Systemeinstellungen

Netzwerkeinstellungen

WLAN Hotspot

Sicherheitseinstellungen

1. SSID	PMA-A1-2.4
2. MAC Address	ec:1a:59:b7:bf:ee
3. Verschlüsselungstyp	AES
4. Network Password	
5. WLAN Repeater SSID	PMA-A1-2.4_28 <input type="checkbox"/> Lokaler Hotspot Freigeben 6.

DHCP Servereinstellungen

7. DHCP Server	<input checked="" type="radio"/> Sperren (empfohlene Konfiguration) <input type="radio"/> Freigeben
----------------	---

Um Netzwerkkonflikte nach der Konfiguration der Parameter zu vermeiden, deaktivieren Sie den DHCP Server.  
Achten Sie sorgfältig darauf, dass die Hotspotparameter richtig und vollständig sind, da das erneute Einloggen nicht funktionieren wird, wenn der DHCP Server deaktiviert ist.

Übernehmen Zurück

1. SSID: Das ausgewählte Netzwerk
  2. MAC Adresse des Routers
  3. Verschlüsselungstyp ist vom Router vorgegeben
  4. Network Password: Passwort des ausgewählten Netzwerkes
  5. WLAN Repeater SSID (greift nur, wenn 6. Aktiviert)
  6. Lokaler Hotspot freigeben: Mit dem Setzen des Hakens, kann ihr Wifi-Modul einen eigenen Hotspot erstellen. Diesen können Sie dann mit einem eigenen Namen versehen.
  7. DHCP Servereinstellungen: Unter diesem Punkt stellen Sie Ihre DHCP Servereinstellung ein. Sie können entweder den Server freigeben oder sperren. Wir empfehlen Ihnen diese Option zu sperren.
- Klicken Sie auf „Übernehmen“, um sich mit dem Router zu verbinden

## Schritt 2b: Erweiterte Einstellungen



Hinweis

Die erweiterten Sicherheitseinstellungen sind nur bei der manuellen Eingabe des Netzwerkes zu sehen.

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen >>

Systemeinstellungen

Netzwerkeinstellungen

WLAN Hotspot

Sicherheitseinstellungen

SSID	PMA-A1-2.4
MAC Address	
Sicherheitsmodus	WPA2-PSK
Verschlüsselungstyp	AES
Network Password	

8.  Synchronisierung der Sicherheitsparameter des Wifi Repeaters mit dem Hotspot

WLAN Repeater SSID: PMA-A1-2.4\_28  Lokaler Hotspot Freigeben

[Erweiterte Einstellungen \(nur für spezifische Anwendungen\) >>](#)

Übernehmen Zurück

- Klicken Sie auf „Erweiterte Einstellungen“, um die verfügbaren Optionen anzuzeigen. Diese Option erlaubt dem FUMO50040 Modul die WLAN-Verbindungen automatisch zu wechseln.
- Wenn Sie wollen, dass das Wifi-Modul dem Netzwerkrouter eine andere SSID übermittelt (er erstellt einen lokalen Hotspot), dann ändern Sie die SSID nach Ihrer Wahl.
- Wenn Sie wollen, dass der eigene Hotspot nicht aktiv ist, dann setzen Sie kein Häkchen bei „lokaler Hotspot freigeben“.

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen >>>

Systemeinstellungen

Netzwerkeinstellungen

WLAN Hotspot

Hotspot Authentifizierungsmodus >>

1.  Vollautomatischer Authentifizierungsmodus (MAC Zertifizierung)

Übernahme von dynamischen Verbindungen des Netzwerks

Verbindungsberechtigte MAC Adressliste +

ff.ff.ff.ff.ff



2.  SSID und Passwort Authentifizierungsmodus

Einstellungen bei Ortsveränderungen <<

3.  Erlaubt Erkennung der Signalstärke während einer Bewegung und verbindet sich mit dem besten Hotspot

Zeitfenster Bewegungserkennung (ms, 500–2000, Standard 2000) (ms, 500–2000, default 2000)

2000

Alarmsignalschwelle (0–90, Standard 40) (0–90, default 40)

40

Signalschwankung (0–20, Standard 10) (0–20, default 10)

10

Übernehmen

Zurück

### 1. Vollautomatischer Authentifizierungsmodus (MAC Zertifizierung):

Das FUMO kann sich mit verschiedenen Geräten, die Geräte in der Liste, (Hotspots) (gleiche SSID und PW) verbinden.

**Hinweis** Das Modul soll sich mit verschiedenen Zugangspunkten (Hotspots) verbinden können. Es soll das jeweils stärkste WLAN Netz genutzt werden. Dazu müssen Sie jeden gewünschten Hotspot auswählen und eine Verbindung aufbauen lassen, weil jeder Hotspot (auch mit gleicher SSID und Passwort) eine andere MAC besitzt.

**Hinweis** Auch die Verwendung von verschiedenen Zugangspunkten (Hotspots) ist möglich. Jeder Hotspot hat seine eigenen SSID und sein eigenes PW. Dazu müssen Sie jeden gewünschten Hotspot auswählen und eine Verbindung aufbauen lassen.

- Setzen Sie den Haken bei „Übernahme von dynamischen Verbindungen des Netzwerks“

**Hinweis** Diese Einstellung wird empfohlen, da sie sicherstellt, die Verbindung aufrechtzuerhalten, insbesondere wenn der Router über Funktionen wie automatische Kanalauswahl und intelligente Kanalauswahl verfügt.

## 2. SSID und Passwort Authentifizierungsmodus

Das FUMO kann sich mit verschiedenen Geräten (gleiche SSID und PW) verbinden.



Hinweis

Diese Einstellung ist hilfreich bei sogenannten Mesh-Netzwerken.

Hier prüft das Modul nicht die MAC Adresse jedes Hotspots.

Sie müssen bei Erweiterungen des WLAN-Netzwerkes keine Initialverbindung zu dem neuen Hotspot etablieren, wie im Vollautomatischen Authentifizierungsmodus (MAC Zertifizierung).

## 3. Einstellungen bei Ortsveränderungen:

Dies sind die Parameter mit dem das Modul entscheidet, wie und wann es sich in ein „besseres“ WLAN Netz einbucht.

Nutzen Sie mehrere Zugangspunkte, dann klicken Sie das Feld an.

Bei Bedarf können Sie jetzt auch die Standardeinstellungen ändern.

- Klicken Sie auf „Übernehmen“, um sich mit dem Router zu verbinden



Hinweis

Beim Hinzufügen von mehreren Netzwerken.

Es erscheint ein Text:

„Wenn Sie einen weiteren Hotspot hinzufügen möchten, klicken Sie bitte auf die Schaltfläche „Weiter hinzufügen“.“

Klicken Sie auf die Schaltfläche "Weiter hinzufügen"

Ergebnis: z.B. werden die Access Points abwechselnd ausgeschaltet, meldet sich das Modul im jeweils anderen Netzwerk an.

- Klicken Sie auf „Neu starten“. Das Wifi-Modul startet neu. Warten Sie in etwa 2 Minuten, schließen Sie das Browser-Fenster und öffnen Sie erneut.
- Machen Sie das Wifi-Modul erneut spannungslos und schließen Sie es wieder an.
- Das Wifi-Modul ist nun mit dem Router verbunden und garantiert eine Internetverbindung an der verbundenen Komponente.

### Schritt 3: Weitere Verbindungen zum Router



Wichtig

Da das Wifi Modul nach der ersten Einrichtung und Verbindung mit dem Heimnetzwerk eine IP-Adresse zugewiesen bekommt, müssen Sie, um wieder auf den Wifi-Adapter zuzugreifen, die IP-Adresse des Wifi-Moduls eingeben.

**Notieren Sie sich also nach der Ersteinrichtung die IP-Adresse des Moduls.**

Die IP Adresse finden Sie auch in der Liste der Netzwerkverbindungen im Router des Kunden

Die Ermittlung der IP-Adresse in dieser Liste stellt sich bei einer größeren Anzahl von Netzwerkkomponenten schwierig dar, da das Modul nur über seine MAC Adresse wieder auffindbar ist. Das Modul erscheint nicht mit seinem Namen in dieser Liste.



## Systemeinstellungen

## Nutzernamenname und Passwort

- Klicken Sie auf „Systemeinstellungen“
- Unter „Anmeldeoptionen“ können Sie den Benutzernamen und das Passwort des FUMO50040 ändern
- Klicken Sie „Übernehmen“, um die Einstellungen zu speichern

Nach Hotspots suchen

Systemeinstellungen >>

Netzwerkeinstellungen

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

ABUS

Betriebsart: WiFi Bridge [English](#)

Anmeldeoptionen | Firmware Upgrade

Errichteroptionen

Benutzername	abus
Passwort	••••
Bestätigen Sie Ihr Passwort	
Hardware Version	VER4.0 (FUMO50040)
Software Version	3.0.17.8.15

Übernehmen Abbrechen



Hinweis

Benutzen Sie sichere Benutzernamen und Codes. Genauere Informationen entnehmen Sie diesbezüglich bitte der Installationsanleitung der Zentrale.

## Firmware Upgrade



Hinweis

Um die Software Version abzuwerten, braucht das Modul eine aktive Internetverbindung und muss zuvor bereits eingerichtet worden sein.

The screenshot shows the ABUS web interface. At the top left is the ABUS logo. At the top right, it says "Betriebsart: WiFi Bridge" and "English". Below the logo, there is a warning message: "Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!". On the left side, there are three menu items: "Nach Hotspots suchen", "Systemeinstellungen >>", and "Netzwerkeinstellungen". The main content area has two tabs: "Anmeldeoptionen" and "Firmware Upgrade". Under the "Firmware Upgrade" tab, there is a section titled "Update Firmware" with three steps: 1. "Update", 2. "Update starten", and 3. "Neustart Gerät".

- Verbinden Sie sich mit der IP-Adresse des Wifi-Moduls und loggen sich über den Webbrowser ein.
- Klicken Sie auf „Systemeinstellungen“ und anschließend auf „Firmware Upgrade“
- Klicken Sie auf „Update“. Der Wifi-Adapter verbindet sich mit dem Server, um die neue Firmware herunterzuladen. Das Wifi-Modul informiert Sie, wenn der Download erfolgreich war
- Klicken Sie auf „Update starten“. Das Wifi-Modul informiert Sie, wenn das Update der neuen Firmware erfolgreich war.
- Klicken Sie auf „Neustart Gerät“, um das Wifi-Modul neu zu starten.



Hinweis

Falls ein Fehler auftritt, wiederholen Sie ihren jeweils letzten Schritt.

## Netzwerk Einstellungen

## Lokaler Netzwerk-Anschlussstyp

Hier können Sie die Netzwerkkonfiguration einstellen. Sie können nun zwischen DHCP oder Statisch auswählen.

## DHCP Modus

The screenshot shows the ABUS web interface for configuring the local network connection type. The 'Lokaler Netzwerk-Anschlussstyp' dropdown menu is highlighted with a red box and is set to 'DHCP (automatische Konfiguration)'. Below this, the 'DHCP Modus' section includes a 'Host Name' field with the value 'abus.com' and a 'DHCP Server' dropdown menu set to 'Sperrern'. At the bottom right of the configuration area, there are two buttons: 'Übernehmen' and 'Abbrechen'. A warning message at the top of the interface states: 'Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!'.

Wenn Sie DHCP auswählen, übernimmt der Router hier die Konfiguration und vergibt automatisch dem Wifi-Modul eine IP-Adresse. Diese können Sie über den Router herausfinden.



## Hinweis

Die Einstellung „gesperrt“ des DHCP-Servers sollte übernommen werden, da sich bei einem Verbindungsabbruch und Wiederverbindung mit dem Router, die IP Adresse des Wifi Modul ändern kann.

## Statischer Modus



Betriebsart: WiFi Bridge [English](#)

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen

Systemeinstellungen

Netzwerkeinstellungen >>

### Lokale IP-Adresse

Lokaler Netzwerk-Anschlussstyp

Verbindungstyp

#### Statischer Modus

IP Adresse	<input type="text" value="192.168.178.226"/>
Subnetzmaske	<input type="text" value="255.255.255.0"/>
Standard Gateway	<input type="text" value="192.168.178.1"/>
Primärer DNS Server	<input type="text" value="192.168.178.1"/>
Sekundärer DNS Server	<input type="text" value="192.168.178.1"/>

DHCP Server

DHCP Server

Übernehmen

Abbrechen

Im statischen Modus werden die Netzwerkkonfigurationen manuell vergeben. Es müssen die Rahmenparameter des verbundenen Netzwerkes übernommen werden. Dazu gehört die Subnetzmaske. Das Standard Gateway und der DNS Server entspricht den IP-Einstellungen des Netzwerkroueters. In der obersten Zeile vergeben Sie de, Wifi Modul eine im Netzwerk noch nicht belegte IP-Adresse. Zum Schluss klicken Sie auf Übernehmen.

## Weitere Informationen zu WLAN und Routern

### Zwei Wi-Fi Access Points mit identischer SSID / identischem Passwort, Administrator

Standardmäßig stellt das Wi-Fi-Modul mit drei verschiedenen Anmeldeinformationen eine Verbindung zu drahtlosen Zugriffspunkten her: der SSID, dem Netzwerkennwort und der MAC-Adresse des Geräts.

Während des Lernvorgangs in der Weboberfläche des Wi-Fi-Moduls wird die SSID mithilfe der Hotspot-Liste aus der Liste der verfügbaren Netzwerke ausgewählt, das Netzwerkennwort vom Techniker eingegeben, der das Wi-Fi-Modul konfiguriert, und die MAC-Adresse wird automatisch extrahiert als Teil dieses Prozesses.

Diese drei Details werden gespeichert, um eine drahtlose Verbindung zum lokalen Netzwerkrouter aufrechtzuerhalten und die Verbindung im Falle einer Unterbrechung wiederherzustellen.

Dies bedeutet, dass, wenn ein Wi-Fi-Modul für ein lokales Netzwerk mit einer festen SSID und einem festen Kennwort konfiguriert ist und anschließend ein zweites Netzwerk mit identischen Anmeldeinformationen erstellt wird, das Wi-Fi-Modul nur mit der MAC-Adresse eine Verbindung zum Zugriffspunkt herstellt, die diese Adresse hat, die mit den Anmeldeinformationen übereinstimmen, die im Rahmen der Konfiguration des Wi-Fi-Moduls gespeichert wurden.

Das Wi-Fi-Modul versucht nicht, eine Verbindung zu einem Zugangspunkt herzustellen, wenn sich die MAC-Adresse, von der während der Konfiguration gespeicherten unterscheidet, unabhängig davon, ob SSID und Netzwerkennwort identisch sind.

Dieses Verhalten kann zu Problemen bei Netzwerken führen, die aus mehreren Repeatern oder Zugangspunkten bestehen, die in der Regel die SSID und das Kennwort ihres Zielnetzwerks wiederholen.

Der vom Wi-Fi-Modul verwendete MAC-Adressmechanismus kann mithilfe der erweiterten Konfigurationsoptionen in der Weboberfläche während der manuellen Konfiguration umgangen werden. Diese erweiterten Einstellungen werden im Dropdown-Menü Hotspot-Authentifizierungs-Übereinstimmungsmodus gespeichert.

Diese erweiterten Optionen sind im normalen Betrieb für das Installationsprogramm nicht sichtbar und werden beim Anmelden an der Weboberfläche mit unterschiedlichen Anmeldeinformationen aufgerufen:

Administratoranmeldeinformationen für FUMO50040:

Benutzername: admin

Passwort: abus

#### Zugriff

Stellen Sie über die Webschnittstelle eine Verbindung zum FUMO50040 her und geben Sie die Administratoranmeldeinformationen anstelle der Benutzeranmeldeinformationen ein (siehe oben). Wählen Sie den gewünschten Zugangspunkt aus der Hotspot-Liste aus, als würden Sie normalerweise ein Wi-Fi-Modul für ein lokales Netzwerk konfigurieren.

Sobald ein Zugangspunkt ausgewählt wurde, öffnet die Weboberfläche die Konfigurationsseite, auf der Sie normalerweise das Netzwerkennwort eingeben. Darunter befindet sich ein gelber Text, in dem ein Dropdown-Menü mit den Einstellungen für den Hotspot-Authentifizierungs-Übereinstimmungsmodus und die Bewegungserkennungsparameter zur Konfiguration verfügbar werden. (siehe unten)

Advanced Setting ( For specific applications only ) <<

Hotspot authentication match mode <<

Fully matched authentication mode(MAC certification)

Allow dynamic match to parameters of hotspots connection

The MAC address list to allow the connection +

18:a6:f7:a9:53:1a -

SSID and password authentication mode(No MAC certification)

Standardmäßig ist die Einstellung vollständig übereinstimmender Authentifizierungsmodus (MAC-Zertifizierung) aktiviert, sodass das Wi-Fi-Modul nur über SSID, Kennwort UND MAC-Adresse eine Verbindung zu konfigurierten Netzwerken herstellen muss.

Dies kann deaktiviert werden, indem die Option SSID- und Kennwortauthentifizierungsmodus (keine MAC-Zertifizierung) ausgewählt wird. Dies bedeutet, dass das Wi-Fi-Modul eine Verbindung zu einem Zugriffspunkt herstellt, der mit einer SSID und einem Kennwort übereinstimmt, für die das Modul konfiguriert wurde (standardmäßig deaktiviert).

## Signalstärke-Entscheidungsfindung

Das Wi-Fi-Modul folgt einem logischen Prozess zur Entscheidung, welcher Zugangspunkt aus der Liste der konfigurierten Zugangspunkte ausgewählt werden soll, wenn zu einem bestimmten Zeitpunkt zwei oder mehr in Reichweite sind. Im Admin-Menü stehen zusätzliche Optionen zur Verfügung, mit denen der Techniker, der das Wi-Fi-Modul konfiguriert, diesen Entscheidungsprozess konfigurieren kann.

Standardmäßig stellt das Wi-Fi-Modul eine Verbindung zum ersten Hotspot her, für den es während des Installationsvorgangs konfiguriert wurde, und bleibt unabhängig von der Signalstärke für diesen Zugriffspunkt konfiguriert, es sei denn, die Verbindung wird getrennt (d.h. der Zugriffspunkt wird ausgeschaltet oder bewegt nach außerhalb der Reichweite des WLAN-Moduls).

Bei einem Verbindungsabbruch versucht das Wi-Fi-Modul, eine Verbindung zu einem anderen konfigurierten Hotspot herzustellen (wenn sich dieser Zugangspunkt in Reichweite befindet), oder es sucht wiederholt nach der unterbrochenen Verbindung des vorheriger Zugangspunkt, mit dem der Wi-Fi-Adapter verbunden war.

Bei einem Aus- und Einschalten, bei dem ein Wi-Fi-Modul für zwei oder mehr verschiedene Zugangspunkte konfiguriert wurde, stellt das Wi-Fi-Modul eine Verbindung mit dem Zugangspunkt her, der zu diesem Zeitpunkt die höchste Signalstärke aufweist, sobald die Wi-Fi-Verbindung hergestellt wurde. Das Modul bleibt mit diesem Zugangspunkt verbunden, bis die Verbindung unterbrochen wird.

Es gibt zusätzliche erweiterte Einstellungen im Menü Bewegungserkennungparameter, mit denen der Techniker das Entscheidungsverhalten für die erneute Verbindung des Wi-Fi-Moduls ändern kann. Standardmäßig sind diese Einstellungen deaktiviert. (siehe unten).

Motion detection parameters <<

Allows detection of signal strength during motion, and connects the best hotspot

Motion detection time window (ms, 500--2000, default 2000) (ms, 500--2000, default 2000)	2000
Signal alarm threshold (0--90, default 40) (0--90, default 40)	40
Signal shake (0--20, default 10) (0--20, default 10)	10

In order to prevent network conflicts, after parameters are configured, please disable DHCP server. Logging in page again will be failed because of 'Disable DHCP server', so please make sure the hotspot parameters are correct.

Apply Back

Bei Auswahl der Option „Erlaubt Erkennung der Signalstärke während einer Bewegung und verbindet sich mit dem besten Hotspot“, kann das Wi-Fi-Modul Verbindungen zwischen konfigurierten Zugriffspunkten abhängig von der Signalstärke wechseln. Die Signalalarmschwelle kann so konfiguriert werden, dass das WLAN-Modul nur eine Verbindung zu einem Access Point herstellt, dessen Signalstärke über der Schwelle liegt.

## DHCP / Feste IP Adresse

DHCP ist der Mechanismus, mit dem ein Router einem Gerät automatisch eine IP-Adresse zuweist. Dies ist die gebräuchlichste Methode für die Zuweisung von IP-Adressen im Privatbereich und eignet sich ideal für Geräte, die öfters eine Verbindung zu einem Netzwerk herstellen und diese auch öfters wieder trennen, z. B. Smartphones.

Feste IP-Adressen sind in kommerziellen Situationen häufiger anzutreffen und eignen sich am besten für Geräte, die nicht aus einem Netzwerk entfernt werden.

Die Secvest Zentralen können sowohl im DHCP- als auch im statischen Modus betrieben werden. Für die beständigste Verbindung empfiehlt ABUS, zunächst DHCP zu verwenden, um die korrekten IP-Adresseinstellungen vom Router zu erhalten. Sobald diese empfangen wurden, sollten sie notiert und in die Zentrale eingegeben werden, um die Zentrale in den statischen IP-Modus zu versetzen.

## Automatische Kanalwahl

Die meisten Router werden standardmäßig mit "automatischer Kanalauswahl" geliefert. Dies bedeutet, dass der Router basierend auf Störungen nach dem besten WLAN-Kanal sucht, um die beste WLAN-Leistung zu erzielen. Im Allgemeinen geschieht dies nur beim Einschalten des Routers.

Einige Router verwenden eine „intelligente automatische Kanalauswahl“. Im Gegensatz zu den meisten automatischen Kanalwahltechniken suchen diese Router ständig nach Störungen - nicht nur von anderen Zugangspunkten, sondern auch von Bluetooth-Geräten und Mikrowellen - und wechselt den Kanal im laufenden Betrieb.

Wenn ein Router den Kanal wechselt, wird zunächst die Verbindung zum WiFi-Modul unterbrochen. Das WiFi-Modul stellt jedoch die Verbindung wieder her und passt sich den vom Router vorgenommenen Änderungen an (Dynamische Anpassung an Parameter der Hotspot-Verbindung zulassen „**Synchronisierung der Sicherheitsparameter des WiFi Repeaters mit dem Hotspot**“ muss im WiFi-Modul aktiviert sein.).

ABUS empfiehlt, das "Smart Wireless Channel-Hopping" im Router zu deaktivieren, um eine möglichst stabile Verbindung herzustellen.

## Bandsteuerung

Einige Dual-Band-Router verwenden eine Technik namens „Bandsteuerung“. Hier wird der Router 2,4 GHz Geräte auf die 5 GHz Frequenz zwingen. Dies liegt daran, dass der 2,4 GHz Frequenzbereich vor allem im Wohnbereich sehr überfüllt ist.

Das WiFi-Modul ist ein 2,4 GHz Gerät.

Wenn ein Router ständig versucht, es auf die 5 GHz Frequenz zu verschieben, wird die Verbindung zum WiFi-Modul unterbrochen.

Um eine möglichst stabile Verbindung zu gewährleisten, empfiehlt ABUS, diese Funktion im Router zu deaktivieren.

## 2.4 GHz and 5 GHz.

Es gibt Dual-Band-Router, d.h. es stehen zwei Funkfrequenzen für Geräte zur Verfügung, mit denen eine Verbindung hergestellt werden kann: 2,4 GHz und 5 GHz. Leider können einige Geräte Schwierigkeiten haben, gleichzeitig mit beiden verbunden zu bleiben, was zu zeitweiliger Unterbrechung der Verbindung oder geringer Leistung führen kann.

In diesem Fall empfiehlt es sich, die beiden Netzwerke aufzuteilen und unterschiedliche Netzwerknamen (SSIDs) für das 2,4 GHz und das 5 GHz Band zu erstellen.

Ändern Sie "Mit 2,4 GHz synchronisieren" in "Nein"

Ändern Sie den Namen der "SSID"

Kurz darauf werden zwei SSIDs in der Liste der Netzwerke auf Ihrem Gerät angezeigt. Das Gerät verbindet sich jetzt automatisch mit der 2,4 GHz Frequenz.

Wenn Sie Dual-Band-Geräte haben, die Sie nur mit 5 GHz verbinden möchten, müssen Sie diese an die 5 GHz-SSID ankoppeln, die Sie umbenannt hatten.



## Gewährleistung



### Hinweis

- ABUS-Produkte sind mit größter Sorgfalt konzipiert, hergestellt und nach geltenden Vorschriften geprüft.
- Die Gewährleistung erstreckt sich ausschließlich auf Mängel, die auf Material- oder Herstellungsfehler zum Verkaufszeitpunkt zurückzuführen sind. Falls nachweislich ein Material- oder Herstellungsfehler vorliegt, wird das Modul nach Ermessen des Gewährleistungsgebers repariert oder ersetzt.
- Die Gewährleistung endet in diesen Fällen mit dem Ablauf der ursprünglichen Gewährleistungszeit von 2 Jahren. Weitergehende Ansprüche sind ausdrücklich ausgeschlossen.
- ABUS haftet nicht für Mängel und Schäden, die durch äußere Einwirkungen (z.B. durch Transport, Gewalteinwirkung, Fehlbedienung), unsachgemäße Anwendung, normalen Verschleiß oder durch Nichtbeachtung dieser Anleitung entstanden sind.
- Bei Geltendmachung eines Gewährleistungsanspruches ist dem zu beanstandenden Produkt der originale Kaufbeleg mit Kaufdatum und eine kurze schriftliche Fehlerbeschreibung beizufügen.
- Sollten Sie an dem Wifi-Modul einen Mangel feststellen, der beim Verkauf bereits vorhanden war, wenden Sie sich innerhalb der ersten zwei Jahre bitte direkt an Ihren Verkäufer.

## Kundendienst und Support

### Endverbraucher

Bei auftretenden Fragen wenden Sie sich bitte an Ihren Fachhändler oder Errichter.

### Fachhändler / Errichter

Bei auftretenden Fragen wenden Sie sich bitte an die entsprechende Support-Hotline.

Informationen zum Produkt finden Sie auf unserer Website.

ABUS Security-Center GmbH & Co. KG

86444 Affing

Linker Kreuthweg 5

GERMANY

[www.abus.com](http://www.abus.com)

[info@abus-sc.com](mailto:info@abus-sc.com)

## Entsorgung



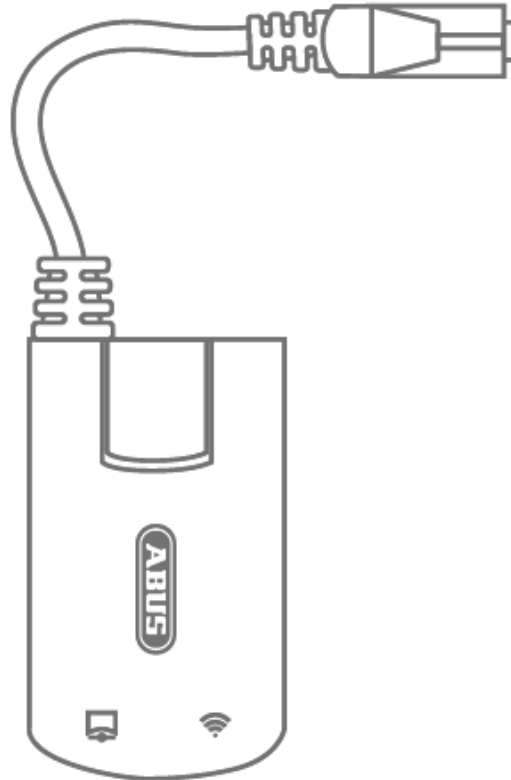
Entsorgen Sie das Gerät gemäß der Elektro- und Elektronik-Altgeräte EU Richtlinie 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). Bei Rückfragen wenden Sie sich an die für die Entsorgung zuständige kommunale Behörde. Informationen zu Rücknahmestellen für Ihre Altgeräte erhalten Sie z.B. bei der örtlichen Gemeinde- bzw. Stadtverwaltung, den örtlichen Müllentsorgungsunternehmen oder bei Ihrem Händler.

## Konformitätserklärung

Hiermit erklärt ABUS Security-Center, dass der Funkanlagentyp FUMO50040 der RED-Richtlinie 2014/53/EU entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter der folgenden Internetadresse verfügbar: [www.abus.com](http://www.abus.com) > Artikelsuche > FUMO50040 > Downloads

Die Konformitätserklärung kann auch unter folgender Adresse bezogen werden:  
ABUS Security-Center GmbH & Co. KG  
Linker Kreuthweg 5  
86444 Affing  
GERMANY

**FUMO50040**  
**Secvest Wi-Fi module**



**DE**

**Secvest WIFI-Modul**

Installations- und Bedienungsanleitung

**EN**

**Secvest Wi-Fi module**

Installation instructions and user manual

## Contents

<b>Inhaltsverzeichnis</b>	<b>2</b>
<b>Einführung</b>	<b>4</b>
Hinweise zur Bedienungsanleitung	4
Bestimmungsgemäße Verwendung	4
Haftungsbeschränkung	4
<b>Sicherheitshinweise</b>	<b>5</b>
Symbolerklärung	5
Verpackung	5
<b>Lieferumfang</b>	<b>5</b>
<b>Technische Daten</b>	<b>6</b>
<b>Funktionsprinzip und Leistungsmerkmale</b>	<b>7</b>
Allgemeines	7
Hauptmerkmale	7
Position und Einbau	7
LEDs	9
Erforderliches Equipment	9
Werkseinstellungen	9
<b>Konfiguration</b>	<b>10</b>
Schritt 1: Einloggen	10
Schritt 2: Erste Verbindung zum Router	11
Schritt 3: Weitere Verbindungen zum Router	16
<b>Systemeinstellungen</b>	<b>17</b>
Nutzernamenname und Passwort	17
Firmware Upgrade	18
<b>Netzwerk Einstellungen</b>	<b>19</b>
Lokaler Netzwerk-Anschlusstyp	19
<b>Weitere Informationen zu WLAN und Routern</b>	<b>21</b>
Zwei Wi-Fi Access Points mit identischer SSID / identischem Passwort, Administrator	21
Signalstärke-Entscheidungsfindung	22
DHCP / Feste IP Adresse	23
Automatische Kanalwahl	23
Bandsteuerung	24
<b>Gewährleistung</b>	<b>25</b>
<b>Kundendienst und Support</b>	<b>25</b>
<b>Entsorgung</b>	<b>26</b>
<b>Konformitätserklärung</b>	<b>26</b>
<b>Contents</b>	<b>28</b>
<b>Introduction</b>	<b>30</b>
Information on user guide	30
Intended use	30
Limitation of liability	30

---

<b>Safety information</b> .....	<b>31</b>
Explanation of symbols.....	31
Packaging.....	31
<b>Scope of delivery</b> .....	<b>31</b>
<b>Technical data</b> .....	<b>32</b>
<b>Functional principle and features</b> .....	<b>33</b>
General.....	33
Main features.....	33
Position and installation.....	33
LEDs.....	35
Required equipment.....	35
Default settings.....	35
<b>Configuration</b> .....	<b>36</b>
Step 1: Logging on.....	36
Step 2: Initial connection to router.....	37
Step 3: Additional connections to the router.....	41
<b>System settings</b> .....	<b>42</b>
User name and password.....	42
Firmware upgrade.....	43
<b>Network settings</b> .....	<b>44</b>
Local network connection type.....	44
<b>More information about Wi-Fi and Routers</b> .....	<b>46</b>
Two Wi-Fi Access Points with Identical SSID/Password, Administrator.....	46
Signal Strength Decision Making.....	47
DHCP / Fixed IP address.....	48
Auto Channel selection.....	48
Band Steering.....	49
<b>Warranty</b> .....	<b>50</b>
<b>Customer service and support</b> .....	<b>50</b>
<b>Disposal</b> .....	<b>51</b>
<b>Declaration of conformity</b> .....	<b>51</b>

## Introduction

### Introduction

### Information on user guide

Dear Customer,

Thank you for purchasing this product. This device is a product that has been built using state-of-the-art technology.

These instructions contain important installation and operation information. Follow the directions and instructions in this user manual to ensure safe operation. Store this manual in a safe place for future reference. This manual constitutes part of the device. If you pass the device on to third parties, please remember to include this manual.

### Intended use

Only use the device for the purpose for which it was built and designed. Any other use is considered unintended. This product complies with current domestic and European regulations.

Conformity has been certified, and all related certifications are available from the manufacturer on request.

To ensure this condition is maintained and that safe operation is guaranteed, it is your obligation as the user to observe this user guide. If you have any questions, please contact your specialist dealer. Further general information and information on product support can be found at [www.abus.com](http://www.abus.com) on the general page or for dealers and installers, in the Partner portal.



#### Note

Please observe the notes and instructions in this user manual! If you do not follow these instructions, any guarantee claim is invalidated. No liability can be accepted for resulting damage.

No part of the product may be changed or modified in any way.

Please observe the local legal requirements. In some European countries, the use of repeaters outdoors is prohibited or the maximum alarm duration is limited. Please consult your local authorities on this.



#### Danger

Set the alarm panel to installer mode before starting any installation or maintenance work. Installer mode prevents alarms from being activated when the repeater's cover is opened.

### Limitation of liability






Everything possible has been done to ensure that the content of these instructions is correct. However, neither the author nor ABUS Security-Center GmbH & Co. KG can be held liable for loss or damage caused by incorrect or improper installation and operation or failure to observe the safety instructions and warnings. No liability can be accepted for resulting damage. No part of the product may be changed or modified in any way. If you do not follow these instructions, your warranty claim becomes invalid. Subject to technical modifications.

© ABUS Security-Center GmbH & Co. KG, 12/2019


## Safety information

### Explanation of symbols

The following symbols are used in this manual and on the device:

Symbol	Signal word	Meaning
	<b>Danger</b>	Indicates a risk of injury or health hazards.
	<b>Danger</b>	Indicates a risk of injury or health hazards caused by electrical voltage.
	<b>Important</b>	Indicates possible damage to the device/accessories.
	<b>Note</b>	Indicates important information.
		The EU Directive WEEE 2012/19/EU governs the proper recovery, treatment and recycling of used electronic devices. This symbol means that, in the interest of environmental protection, the device must be disposed of separately from household or industrial waste at the end of its lifespan in accordance with applicable local legal guidelines. Used devices can be disposed of at official recycling centres in your country. Obey local regulations when disposing of materials. Further details on returns (also for non-EU countries) can be obtained from your local authority. Separate collection and recycling conserve natural resources and ensure that all the provisions for protecting health and the environment are observed when recycling the product.

## Packaging

 Danger	Keep packaging material and small parts away from children. There is a risk of suffocation.
	Remove all packaging material before using the device.

## Scope of delivery

- 1X ABUS Wi-Fi module
- 1x DC-DC converter
- 1x Quick Guide
- 1x Safety instructions
- Installation material

## Technical data

---

### Technical data

Product name	ABUS Wi-Fi Module
Product description	Wi-Fi module
Item number	FUMO50040
Manufacturer	ABUS Security-Center GmbH & Co. KG
Supported network encryption	54/128/WEP encryption; WPA-PSK/WPA2-PSK, WPA/WPA2
Operating band	2.4 GHz
Transmission speed	Max. 300 Mbps
Ethernet cable length	150 mm
Wireless	2.4 GHz; 100 mW max.
Operating temperature	-10°C to +55°C
Humidity, maximum	Max. 93%, non-condensing
Dimensions (W x H x D)	350 x 590x 110 mm
Weight	20 g (Wi-Fi module), 22 g (DC converter)
Power supply type	Cable type W (EN 50131-4:2009 Section 5.6.3.2)
Power consumption/energy consumption	Max. 220 mA @ 5 V DC
Operating voltage	5 V DC
DC converter	Input: Power input max. 100 mA @ 12 V DC Output: max. 22 D mA @ max. 5 V DC



## Functional principle and features

### General

The FUMO50040 Wi-Fi module allows the connection of ABUS alarm panels to a local network router via a wireless network. A direct Ethernet cable connection between alarm panels and local network routers is therefore no longer required. The Wi-Fi module is supplied with power directly via the alarm panel and installed within the housing.

### Main features

Compatible with Secvest alarm panels	Installed directly insider the Secvest housing
Functions as a connection between the domestic router, thus replacing the connection via an Ethernet cable	Not battery-operated

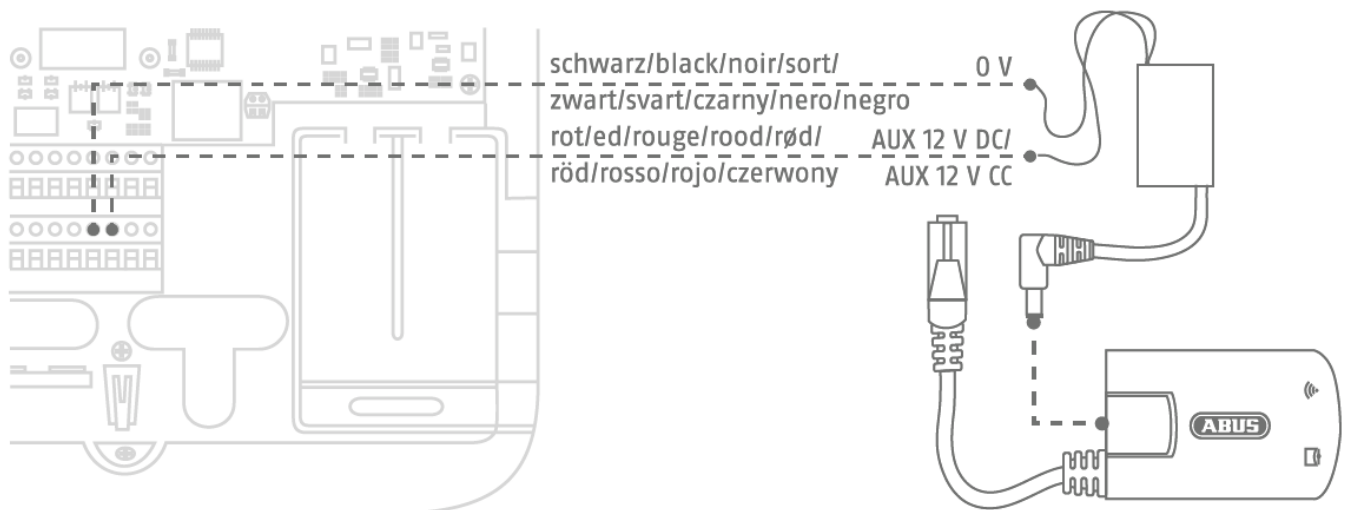


Danger

- Switch the Secvest alarm panel to installer mode and completely disconnect the system from a power source before starting any installation or maintenance work.

### Position and installation

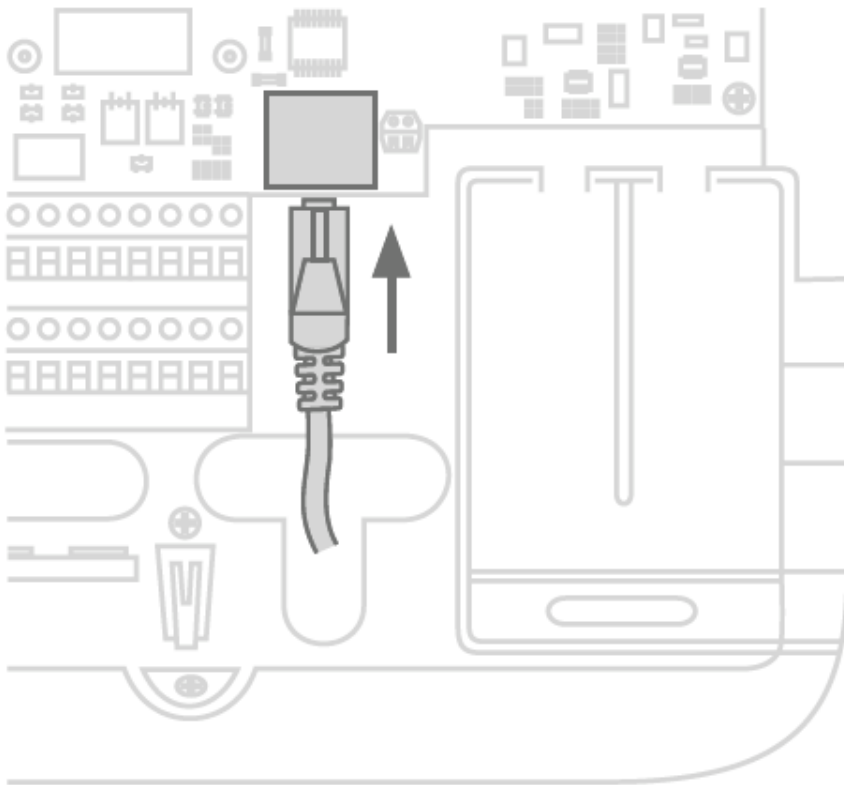
1. Connect the DC-DC converter to the Wi-Fi module. Then connect the black and the red cables as illustrated in the following diagram.



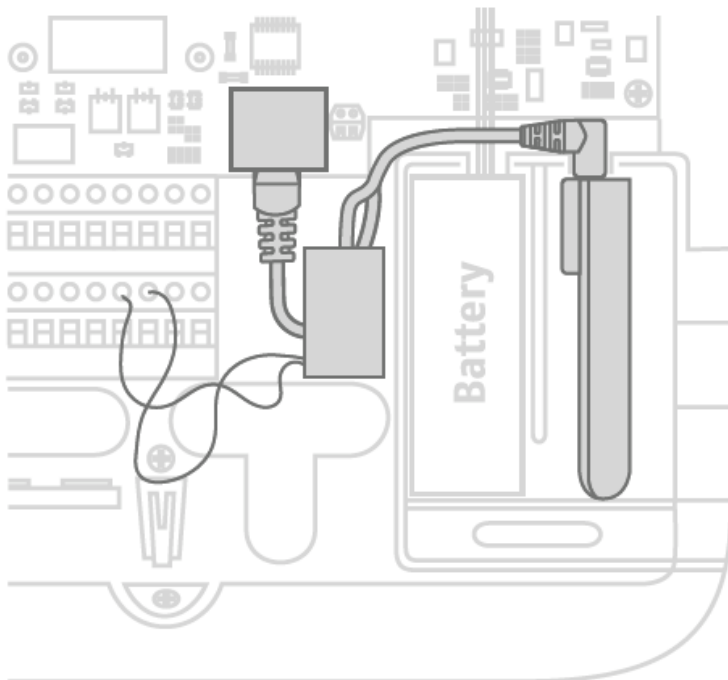
Note

The module should be mounted near a heat source.

### 2. Connect the Wi-Fi module's Ethernet cable



### 3. Position the Wi-Fi module and the converter near the Ethernet connection in the Secvest. The following diagram illustrates one possible position.



### LEDs

Rapidly flashing blue LEDs	Wi-Fi connection to router OK
Slowly flashing blue LEDs	Wi-Fi connection to router not OK
Flashing green LEDs	Ethernet connection

### Required equipment

The following is required to program the FUMO50040 Wi-Fi module:

- A Wi-Fi-enabled laptop, smartphone or tablet
- The customer's Wi-Fi password in order to connect to the module



Note

If there are several Wi-Fi repeaters inside the property, please switch these off before connecting the FUMO50040 Wi-Fi adapter to the main router



Note

Please check whether the FUMO50040 Wi-Fi adapter is compatible with your router (Sky Q routers are not compatible)

If the FUMO50040 Wi-Fi adapter is not compatible with the router, please connect the alarm panel directly to the router by means of an Ethernet cable

### Default settings

- Disconnect the Wi-Fi module from the power supply
- Press the "Reset" button on the flat upper surface of the module. Keep this pressed down
- Reconnect the Wi-Fi module to the power
- Wait for approx. 30 seconds until the LED flashes blue and only then release the "Reset" button
- The device will restart. This takes around 2 minutes

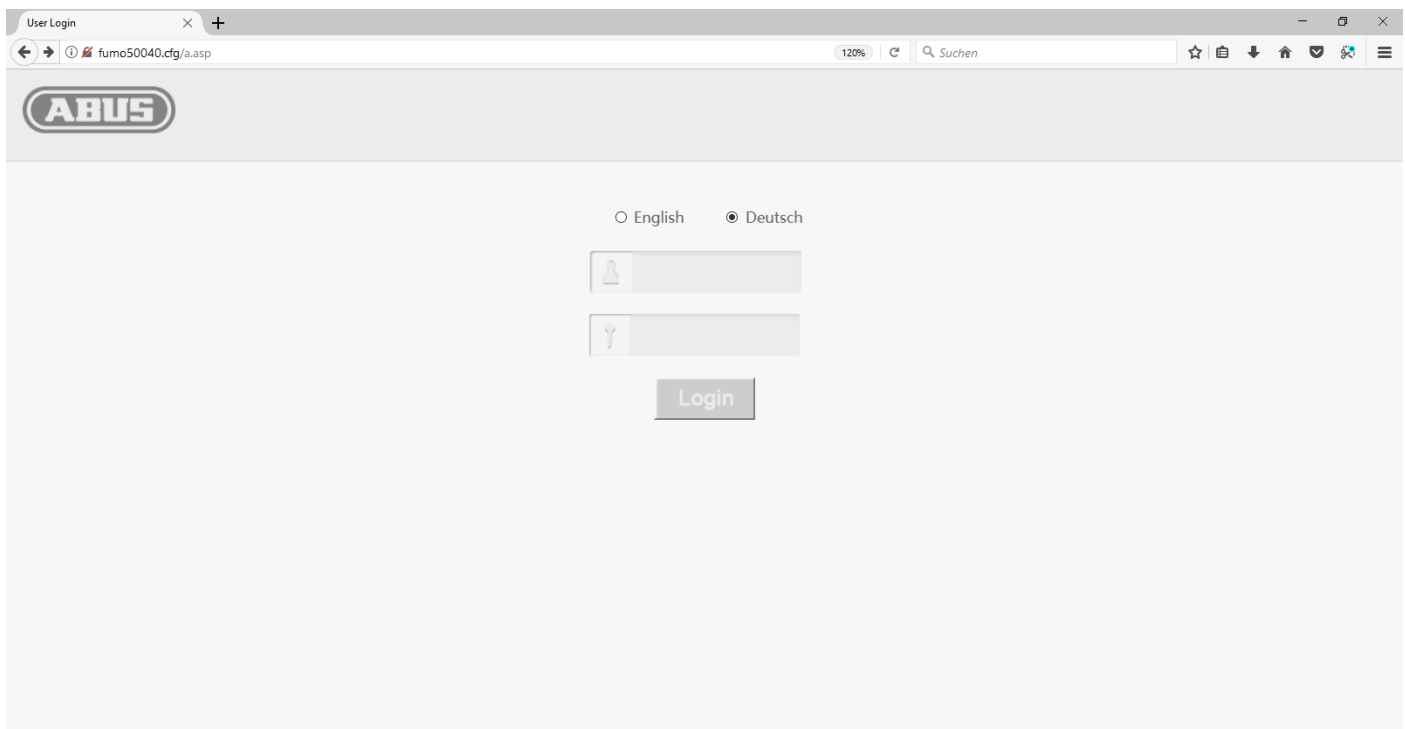
### Configuration

#### Step 1: Logging on

- A Wi-Fi-enabled laptop or another Wi-Fi-enabled device is required
- Go to the network settings and connect to the “FUMO50040” network
- The default password is “12345678”.



- Open the Internet browser and enter <http://fumo50040.cfg> in the address line at the top. You will be taken to the Wi-Fi module login page
- Log in with the user name “abus” and the password “abus”
- Click on “Login”



## Step 2: Initial connection to router

- Click on “Search for hotspots” in the menu options.
- Select the customer’s Wi-Fi network from the list
- Click on “Next”



Note

If there are several Wi-Fi repeaters inside the property, please switch these off before connecting the FUMO50040 Wi-Fi module to the main router

ABUS Betriebsart: Wi-Fi Bridge English

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen >>

Systemeinstellungen

Netzwerkeinstellungen

### WLAN Hotspot

Wählen Sie eine Netzwerk aus, um sich mit diesem zu verbinden. Wenn das gewünschte Netzwerk nicht gefunden wird, laden Sie die Seite erneut oder geben Sie die SSID manuell ein. Danach auf “Weiter” klicken.

SSID	MAC	Kanal	Signal	Auth / Enc
PMV_Video - Retail	02:1d:aa:b3:ed:48	12	100	WPA2-PSK / AES
WLAN-ASC	02:a0:57:1b:eb:00	8	96	WPA2 / AES
WLAN-Gast	00:a0:57:1b:eb:00	8	96	WPA2-PSK / AES
PMA-A1-2.4	ec:1a:59:b7:bf:ee	1	96	WPA2-PSK / AES
PMV_Testlabor	00:1d:aa:b3:ed:48	12	91	WPAPSK-WPA2PSK / TKIPAES
PMV_Testlabor_2EX	74:da:38:c0:55:a8	12	86	WPA2-PSK / AES
WLAN-Gast	00:a0:57:1b:f2:de	6	86	WPA2-PSK / AES
WLAN-ASC	02:a0:57:1b:f2:de	6	86	WPA2 / AES

Es gibt 15 Netzwerke

SSID

Liste neu laden

Weiter Beenden

- If the router’s network does not appear in the list, click on menu option “SSID” (marked in red on image above)
- Enter the network manually



Note

With the manual entry of a network from the list you also get to the advanced settings. See configuration step 2b

- Click on “Next”

### Step 2a: Security settings



#### Note

This view can be seen when selecting the network from the list.

- After clicking “Next”, the security settings will appear.
- Enter the network password for the home router (point 4).

The screenshot shows the ABUS configuration interface for a WLAN Hotspot. The interface is in German and includes a navigation menu on the left with options: "Nach Hotspots suchen", "Systemeinstellungen", and "Netzwerkeinstellungen". The main content area is titled "WLAN Hotspot" and contains two sections: "Sicherheitseinstellungen" and "DHCP Servereinstellungen".

**Sicherheitseinstellungen**

1. SSID	PMA-A1-2.4
2. MAC Address	ec:1a:59:b7:bf:ee
3. Verschlüsselungstyp	AES
4. Network Password	
5. WLAN Repeater SSID	PMA-A1-2.4_28
<input type="checkbox"/> Lokaler Hotspot Freigeben <b>6.</b>	

**DHCP Servereinstellungen**

7. DHCP Server	<input checked="" type="radio"/> Sperren (empfohlene Konfiguration) <input type="radio"/> Freigeben
----------------	---

Um Netzwerkkonflikte nach der Konfiguration der Parameter zu vermeiden, deaktivieren Sie den DHCP Server.  
Achten Sie sorgfältig darauf, dass die Hotspotparameter richtig und vollständig sind, da das erneute Einloggen nicht funktionieren wird, wenn der DHCP Server deaktiviert ist.

Buttons: Übernehmen, Zurück

- 1) SSID: The selected network
  - 2) MAC address of the router
  - 3) The encryption type is specified by the router
  - 4) Network password: Password for the selected network
  - 5) Wi-Fi repeater SSID (only selected when point 6 is enabled)
  - 6) Local hotspot enabled: Ticking the box enables your Wi-Fi module to create its own hotspot. You can then give this a name.
  - 7) DHCP server settings: You can adjust your DHCP server settings in this section. You can either enable or disable the server. We recommend disabling this option.
- Click “Accept” to connect to the router

Step 2b: Advanced settings



The advanced security settings can only be seen when inputting the network manually.

- Click “Advanced settings” to display the available options. This option allows the FUMO50040 module to switch Wi-Fi connections automatically.
- If you want the Wi-Fi module to transmit another SSID to the network router (it will create a local hotspot), change the SSID to the one you want.
- If you do not want the hotspot to be active, do not tick the box for “Local hotspot enabled”.

1)

Fully automatic authentication mode:

The FUMO can be connected to various devices, the devices in the list, (hotspots) (same SSID and PW).



Note

The module should be able to connect to different access points (hotspots). The strongest WiFi network should be used.

To do this, you have to select each desired hotspot and have a connection established because each hotspot (even with the same SSID and password) has a different MAC.



Note

It is also possible to use different access points (hotspots).

Each hotspot has its own SSID and PW.

To do this, you must select any hotspot you want and have a connection established.

- Tick the box for “Allow dynamic match to parameters of hotspot connection”



Note

This setting is recommended because it ensures that the connection is maintained, in particular when the router has functions such as automatic channel selection and intelligent channel selection.

2)

SSID and password authentication mode

The FUMO can be connected to various devices (same SSID and PW); the devices in the list are explicit exceptions.



Note

This setting is helpful for so-called mesh networks.

Here the module does not check the MAC address of each hotspot.

You do not have to establish an initial connection to the new hotspot when expanding the WLAN network, as in the fully automatic authentication mode (MAC certification).

3)

Settings for changes of location: There is no function allocated to this point. We therefore recommend ignoring this and not clicking on it

These are the parameters with which the module decides how and when it logs into a "better" WLAN network.

If you use several access points, click on the field.

You can now change the default settings if necessary.

- Click “Accept” to connect to the router





## Note

When adding multiple networks.

it appears:

**„If you want to add one more hotspot, please click “Continue Add” button”**  
click “continue Add” button

Result: e.g. if the access points are switched off alternately, the module logs into the respective other network.

- Click on “Restart”. The Wi-Fi module will restart. Wait for around 2 minutes, then close and reopen the browser window.
- De-energize the Wifi module and reconnect it.
- The Wi-Fi module is now connected to the router and guarantees an Internet connection to the connected components.

### Step 3: Additional connections to the router



## Important

Because the Wi-Fi module is assigned an IP address after the initial set-up and connection to the home network, you will have to enter the Wi-Fi module’s IP address in order to regain access to the Wi-Fi adapter.

So, after the initial setup, write down the module's IP address.

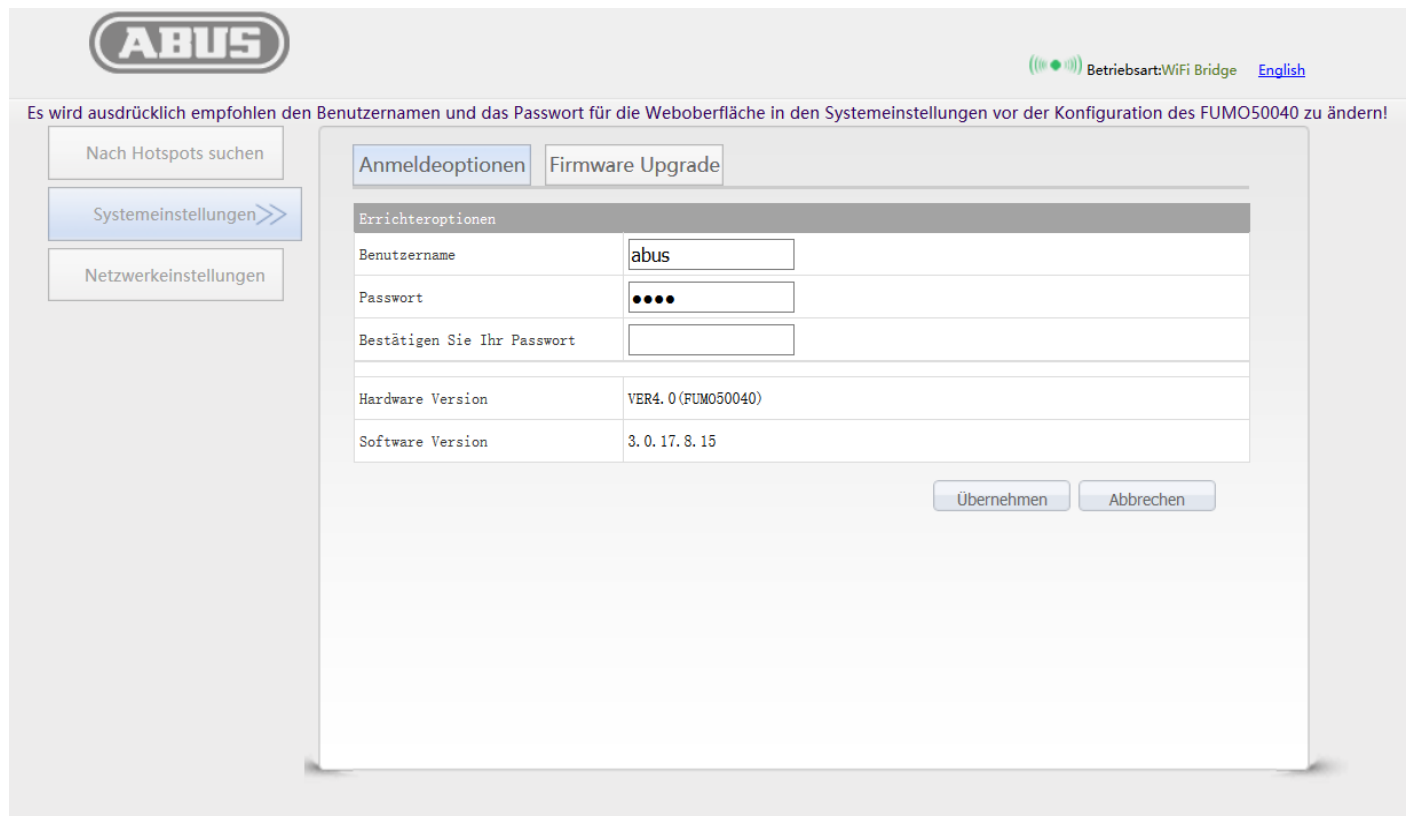
The IP address can also be found in the list of network connections in the customer's router

The determination of the IP address in this list is difficult for a large number of network components, since the module can only be found again via its MAC address. The module does not appear in this list with its name.

### System settings

#### User name and password

- Click on “System Settings”
- You can change the user name and password for the FUMO50040 module under “Login Settings”
- Click “Accept” to save the settings



The screenshot shows the ABUS web interface. At the top left is the ABUS logo. At the top right, it says "Betriebsart: WiFi Bridge" and "English". Below the logo, there is a warning message: "Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!". On the left side, there are three buttons: "Nach Hotspots suchen", "Systemeinstellungen >>" (highlighted), and "Netzwerkeinstellungen". The main content area has two tabs: "Anmeldeoptionen" (selected) and "Firmware Upgrade". Under "Anmeldeoptionen", there is a section titled "Errichteroptionen" containing a form with the following fields:

Benutzername	abus
Passwort	••••
Bestätigen Sie Ihr Passwort	
Hardware Version	VER4.0 (FUMO50040)
Software Version	3.0.17.8.15

At the bottom right of the form, there are two buttons: "Übernehmen" and "Abbrechen".



#### Note

Use secure user names and passwords. For more detailed information, please refer to the alarm panel installation instructions.

## Firmware upgrade



## Note

In order to upgrade the software version, the module requires an active internet connection and must have already been set up.

- Connect using the Wi-Fi module IP address and log in via the web browser.
- Click “System Settings” and then “Firmware Upgrade”
- Click on “Update”. The Wi-Fi adapter connects to the server in order to download the new firmware. The Wi-Fi module will inform you when the download has been completed successfully.
- Click on “Start update”. The Wi-Fi module will inform you when the firmware update has been completed successfully.
- Click “Reboot device” to reboot the Wi-Fi module.



## Note

If an error occurs, repeat the last step.

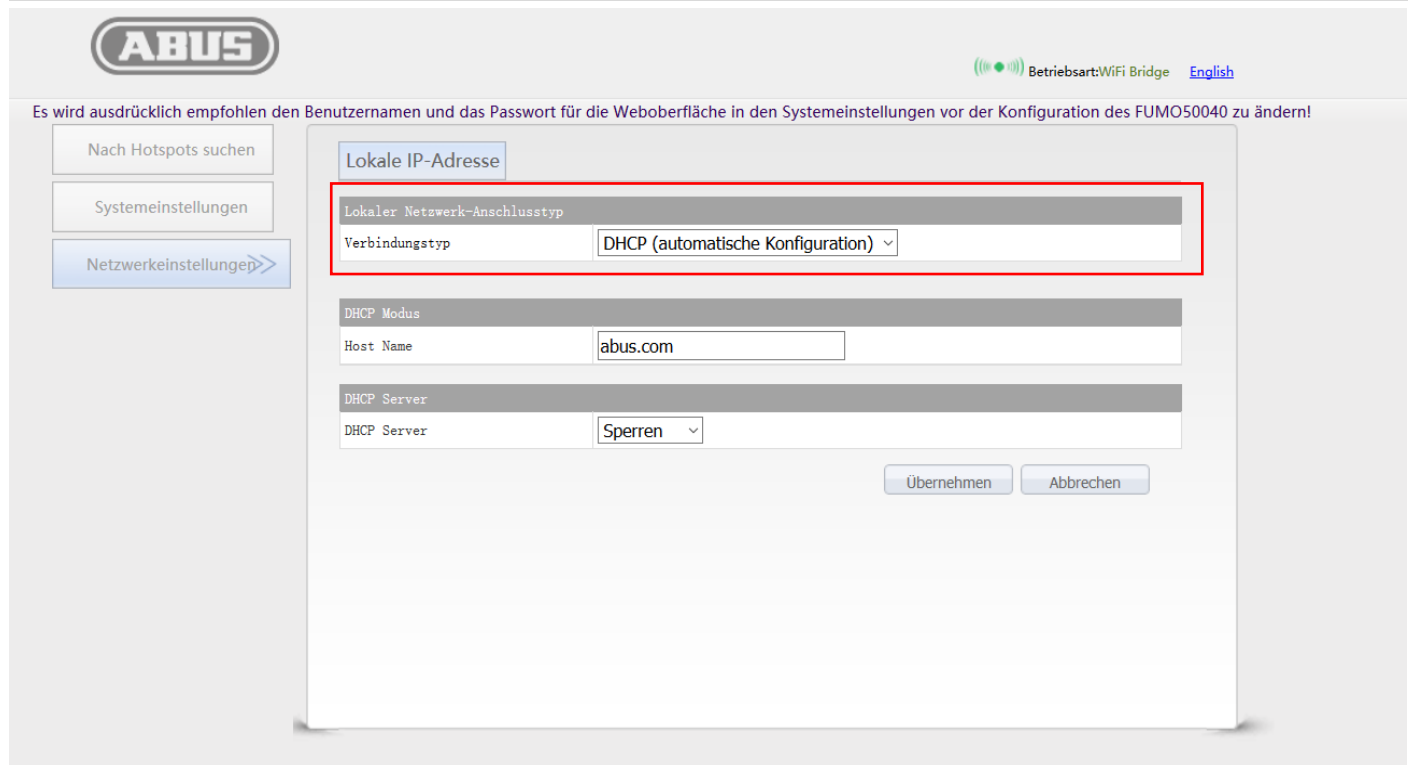
## Network settings

### Network settings

#### Local network connection type

Here the network configuration can be adjusted to either DHCP or static.

#### DHCP mode



The screenshot shows the ABUS web interface for configuring network settings. The page title is "Lokale IP-Adresse". The "Verbindungstyp" (Connection type) is set to "DHCP (automatische Konfiguration)". The "Host Name" is set to "abus.com". The "DHCP Server" is set to "Sperrten". The "Übernehmen" (Apply) and "Abbrechen" (Cancel) buttons are visible at the bottom right of the configuration area.

ABUS

Betriebsart: WiFi Bridge English

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen

Systemeinstellungen

Netzwerkeinstellungen >>

Lokale IP-Adresse

Lokaler Netzwerk-Anschlusstyp

Verbindungstyp

DHCP Modus

Host Name

DHCP Server

DHCP Server

Übernehmen Abbrechen

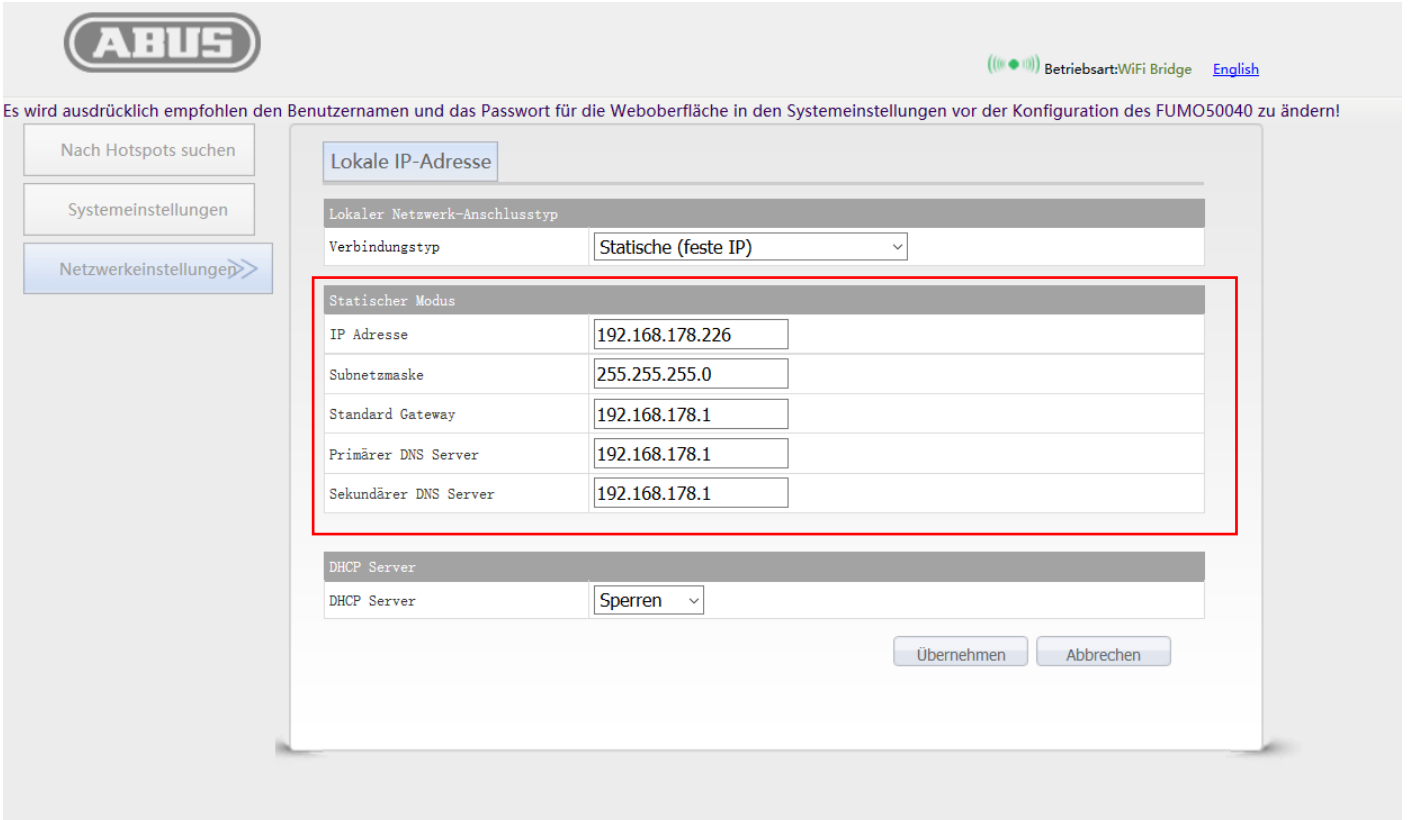
If you select DHCP, the router will adopt the configuration and automatically assign the Wi-Fi module an IP address, which can be found out from the router.



Note

The DHCP server "disabled" setting should be accepted because losing and re-establishing the connection with the router can alter the Wi-Fi module's IP address.

## Static mode



ABUS

Betriebsart: WiFi Bridge English

Es wird ausdrücklich empfohlen den Benutzernamen und das Passwort für die Weboberfläche in den Systemeinstellungen vor der Konfiguration des FUMO50040 zu ändern!

Nach Hotspots suchen

Systemeinstellungen

Netzwerkeinstellungen >>

Lokale IP-Adresse

Lokaler Netzwerk-Anschlusstyp

Verbindungstyp Statische (feste IP)

Statischer Modus

IP Adresse	192.168.178.226
Subnetzmaske	255.255.255.0
Standard Gateway	192.168.178.1
Primärer DNS Server	192.168.178.1
Sekundärer DNS Server	192.168.178.1

DHCP Server

DHCP Server Sperren

Übernehmen Abbrechen

In static mode, the network configurations are entered manually. The framework parameters of the connected network must be adopted. This includes the subnet mask. The default gateway and DNS server correspond to the IP settings of the network router. In the top line, allocate an IP address that has not yet been assigned within the network. Then click "Accept".

### More information about Wi-Fi and Routers

#### Two Wi-Fi Access Points with Identical SSID/Password, Administrator

By default, the Wi-Fi module connects to wireless access points using three different credentials: the SSID, the network password and the device MAC address.

During the learning process in the Wi-Fi module web interface, the SSID is selected from the list of available networks using the hotspot list, the network password is entered by the engineer configuring the Wi-Fi module and the MAC address is automatically extracted as part of this process.

These three details are stored for retaining a wireless connection with the local network router and reconnecting in the event of a disconnect.

This means that if a Wi-Fi module is configured for a local network with a fixed SSID and password, and a second network is then created with identical credentials, the Wi-Fi module will only connect to the access point with the MAC address that matches the credentials saved as part of the Wi-Fi module configuration.

The Wi-Fi module will not attempt to connect to an access point if the MAC address is different to any saved during configuration, regardless if the SSID and network password is identical.

This behaviour potentially causes issues for networks that consist of multiple repeaters or range extender devices that typically repeat or mimic the SSID and password of their target network.

The MAC address mechanism used by the Wi-Fi module can be bypassed using advanced configuration options in the web interface during manual configuration, these advanced settings are stored under the drop-down menu **Hotspot Authentication Match Mode**.

These advanced options are hidden from the installer during normal operation and are accessed using different credentials when logging into the web interface:

#### **FUMO50040 Administrator Credentials:**

Username: **admin**

Password: **abus**

**i**

#### **How to Access**

Connect to the FUMO50040 device via the web interface and enter the administrator credentials instead of the user credentials (see above).

Select the desired access point from the hotspots list as you would if normally configuring a Wi-Fi module for a local network.

Once an access point has been selected, the web interface will open the configuration page where you would normally enter the network password, below this there will be some yellow text that hides a dropdown menu where the Hotspot Authentication Match Mode and Motion Detection Parameter settings are available for configuration. (see below)

Advanced Setting ( For specific applications only ) <<

Hotspot authentication match mode <<

Fully matched authentication mode (MAC certification)

Allow dynamic match to parameters of hotspots connection

The MAC address list to allow the connection +

18:a6:f7:a9:53:1a -

SSID and password authentication mode (No MAC certification)

By default, the setting **Fully matched authentication mode (MAC certification)** is enabled, forcing the Wi-Fi module to only connect to configured networks by SSID, password **AND** MAC address.

This can be disabled by selecting the option **SSID and password authentication mode (No MAC certification)**, meaning the Wi-Fi module will connect to any access point that matches an SSID and password the module has been configured for (disabled by default).

## Signal Strength Decision Making

The Wi-Fi module follows a logical process for deciding which access point from the list of configured access points if there are two or more available in range at any given time. There are additional options available within the admin menu that allow the engineer configuring the Wi-Fi module to configure this decision-making process.

By default, the Wi-Fi module will connect to the first hotspot it is configured for during the setup process and will remain configured to that access point regardless of signal strength unless there is a disconnect (i.e. the access point is powered down or is moved out of range of the Wi-Fi module).

In the event of a disconnect, the Wi-Fi module will try to connect to another hotspot that it has been configured (if this access point is in range), or it will repeatedly search for and try to reconnect with the lost connection of the previous access point the Wi-Fi adapter was connected to. In the event of a power cycle where a Wi-Fi module has been configured for two or more different access points, the Wi-Fi module will connect to the access point with the greatest signal strength level at that time, once connected the Wi-Fi module will remain connected to this access point until the connection is lost.

There are additional advanced settings under the menu **Motion Detection Parameters** that allow the engineer to alter the reconnection decision making behaviour of the Wi-Fi module, by default these settings are disabled. (see below).

Motion detection parameters <<

Allows detection of signal strength during motion, and connects the best hotspot

Motion detection time window (ms, 500--2000, default 2000) (ms, 500--2000, default 2000)	2000
Signal alarm threshold (0--90, default 40) (0--90, default 40)	40
Signal shake (0--20, default 10) (0--20, default 10)	10

In order to prevent network conflicts, after parameters are configured, please disable DHCP server. Logging in page again will be failed because of 'Disable DHCP server', so please make sure the hotspot parameters are correct.

Apply Back

Selecting the option **Allows detection of signal strength during motion, and connects the best hotspot** allows the Wi-Fi module to swap connections between configured access points depending on the signal strength level. The signal alarm threshold can be configured so that the Wi-Fi module will only connect to an access point with a signal strength above the threshold.

### DHCP / Fixed IP address

DHCP is the mechanism for a router to automatically issue an IP address to a device, this is the most common method of IP address allocation in the residential sector and is ideally suited for devices that connect and disconnect from a network such as smartphones.

Fixed IP addresses are more common in commercial situations and are best suited for devices that are not removed from a network.

The Secvest panels can operate in both DHCP and Static mode. For the most consistent connection ABUS recommends using DHCP initially to gain the correct IP address settings from the router, once received these should be noted down then entered in the panel to place the panel into Static IP mode.

### Auto Channel selection

Most routers come default as "auto channel selection", this means the router will scan for the best Wi-Fi channel based on interference to provide the best Wi-Fi performance. Generally, this only happens on power up of the router.

Some routers employ "smart auto channel selection" such as the BT home hubs. Unlike most automatic channel selection techniques, BT's constantly checks for interference - not just from other access points but also from Bluetooth devices and microwaves - and changes channel on the fly. If a router changes channel then this will initially break the connection to the WiFi-module, however the WiFi-module will reconnect and match the changes made by the router ("Allow dynamic match to parameters of hotspots connection" must be enabled in the WiFi-module).

ABUS suggest disabling the " Smart Wireless channel-hopping" in the router for the most stable connection.



### Band Steering

Some Dual band routers employ a technique called “Band Steering” this is where the router will force 2.4 GHz devices on to the 5GHz frequency, this is because the 2.4 GHz has been very congested particularly in the residential market.

The WiFi-module is a 2.4 GHz device, if a router is continually attempting to move it to the 5 GHz frequency then this will break the connection to the WiFi-module.

To ensure the most stable connection, ABUS recommend disabling this type of feature in the router.

### 2.4GHz and 5GHz.

There is a dual band router, which means that there are two wireless frequencies for devices to connect to: 2.4GHz and 5GHz. Unfortunately, some devices can struggle to remain connected to both at the same time, which can result in intermittent connectivity or slow performance.

In this case, it may be best to split out the two networks and create different network names (SSIDs) for the 2.4 GHz and the 5 GHz bands.

Change “Sync with 2.4Ghz” to No

Change the name of the “Wireless SSID”

Two SSIDs will soon appear in the list of networks on your device, which will automatically connect to the 2.4GHz frequency. If you have existing dual band devices you want to connect to 5GHz only, you'll need to hook them up to the 5GHz SSID that you've renamed.

### Warranty



#### Note

- ABUS products are designed and manufactured with the greatest care and tested according to the applicable regulations.
- The warranty only covers defects caused by material or manufacturing errors at the time of sale. If there are demonstrable material or manufacturing errors, the module will be repaired or replaced at the guarantor's discretion.
- In such cases, the warranty ends when the original warranty period of two years expires. All further claims are expressly rejected.
- ABUS will not be held liable for defects and damage caused by external influences (e.g. transport, use of force, operating errors), inappropriate use, normal wear and tear or failure to observe the instructions in this manual.
- In the event of a warranty claim, the original proof of purchase with the date of purchase and a short written description of the problem must be supplied with the product.
- If you discover a defect with your Wi-Fi module that existed at the time of purchase, contact your dealer directly within the first two years.

### Customer service and support

#### End consumer

Please consult your dealer or installer if you have any questions.

#### Dealer/installer

In case of questions, please contact the appropriate support hotline.

Consult our website for product information.

ABUS Security-Center GmbH & Co. KG

86444 Affing

Linker Kreuthweg 5

GERMANY

[www.abus.com](http://www.abus.com)

[info@abus-sc.com](mailto:info@abus-sc.com)

## Disposal



Dispose of the device in accordance with EU Directive 2012/19/EU – WEEE (Waste Electrical and Electronic Equipment). If you have any questions, please contact the municipal authority responsible for disposal. You can get information on collection points for waste equipment from your local authority, from local waste disposal companies or your dealer, for example.

## Declaration of conformity

ABUS Security-Center hereby declares that the radio system type FUMO50040 complies with RED Directive 2014/53/EU. The full EU Declaration of Conformity text can be found at: [www.abus.com](http://www.abus.com) > Item search > FUMO50040 > Downloads

The Declaration of Conformity can also be obtained from the following address:

ABUS Security-Center GmbH & Co. KG  
Linker Kreuthweg 5  
86444 Affing  
GERMANY